VPLS BGP Signaling L2VPN Inter-AS Option B

The VPLS BGP Signaling L2VPN Inter-AS Option B feature simplifies the auto-discovery and signaling of all known provider edge (PE) devices in a Virtual Private LAN Switching (VPLS) instance by using Border Gateway Protocol (BGP). This document describes how to configure the VPLS BGP Signaling L2VPN Inter-AS Option B feature.

• Finding Feature Information, on page 1
• Prerequisites for VPLS BGP Signaling L2VPN Inter-AS Option B, on page 1
• Information About VPLS BGP Signaling L2VPN Inter-AS Option B, on page 2
• How to Configure VPLS BGP Signaling L2VPN Inter-AS Option B, on page 3
• Configuration Examples for L2VPN VPLS Inter-AS Option B, on page 8
• Additional References for VPLS BGP Signaling L2VPN Inter-AS Option B, on page 13
• Feature Information for VPLS BGP Signaling L2VPN Inter-AS Option B, on page 14

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for VPLS BGP Signaling L2VPN Inter-AS Option B

• Disable control word for Virtual Private LAN Switching (VPLS) Border Gateway Protocol (BGP) signaling by using the no control-word command under a pseudowire class. For example:

  Device> enable
  Device# configure terminal
  Device(config)# pseudowire-class my-pw-class
  Device(config-pw-class)# no control-word
The route distinguisher (RD) must match for all the virtual forwarding instances (VFIs) in a VPLS domain.

Ensure that the L2VPN VPLS Inter-AS Option B feature is configured on Autonomous System Boundary Routers (ASBRs) and PE devices.

Information About VPLS BGP Signaling L2VPN Inter-AS Option B

BGP Auto-discovery and Signaling for VPLS

The Virtual Private LAN Switching (VPLS) control plane is used for auto-discovery and signaling. Auto-discovery involves locating all provider edge (PE) devices that participate in a particular VPLS instance. Signaling is accomplished by configuring pseudowires for a VPLS instance. Prior to the introduction of the VPLS BGP Signaling L2VPN Inter-AS Option B feature, Label Distribution Protocol (LDP) was used for signaling and Border Gateway Protocol (BGP) was used for auto-discovery, as specified in RFC 6074. With the introduction of the VPLS BGP Signaling L2VPN Inter-AS Option B feature, the VPLS BGP Signaling L2VPN feature supports RFC 4761 by simplifying the auto-discovery and signaling of all known PE devices in a VPLS instance by using BGP for both functions. Auto-discovery is defined per VPLS instance.

Internal BGP (IBGP) peers exchange update messages of the L2VPN Address Family Identifier (AFI) and the Subsequent Address Family Identifier (SAFI) numbers with L2VPN information to perform both auto-discovery and signaling, which includes the Network Layer Reachability Information (NLRI).

Both BGP standards (RFC 6074 and RFC 4761) for the auto-discovery protocol for VPLS use the same BGP AFI (25) and SAFI (65) but they have different Network Layer Reachability Information (NLRI) encoding, which makes them incompatible with each other. CLI configuration is needed to distinguish the two encoding types as they are mutually exclusive per neighbor. The difference between the two BGP standards is:

- RFC 6074 provides guidelines for specifying length encoding as bits.
- RFC 4761 provides guidelines for specifying length encoding as bytes.

To detect which NLRI encoding standard is supported, the length encoding needs to be determined.

BGP L2VPN Signaling with NLRI

Network Layer Reachability Information (NLRI) enables Border Gateway Protocol (BGP) to carry supernetting information, as well as perform aggregation. Each NLRI consists of block labels that follow the structure LB, LB+1, ..., LB+VBS-1. The NLRI is exchanged between BGP devices for BGP auto-discovery with BGP signaling. The following fields are configured or auto-generated for each Virtual Private LAN Switching (VPLS) instance:

- Length (2 Octets)
- Route distinguisher (RD) is usually an auto-generated 8-byte VPN ID that can also be configured. This value must be unique for a VPLS bridge-domain (or instance).
- VPLS Endpoint ID (VEID) (2 Octets). Each PE device is configured with a VEID value.
How to Configure VPLS BGP Signaling L2VPN Inter-AS Option B

Enabling BGP Auto-discovery and BGP Signaling

Perform this task to enable Virtual Private LAN Service (VPLS) PE devices to discover other PE devices by BGP auto-discovery and BGP signaling functions announced through I.BGP.

SUMMARY STEPS

1. enable
2. configure terminal
3. l2vpn vfi context vfi-context-name
4. vpn id vpn-id
5. autodiscovery bgp signaling bgp
6. ve id ve-ID-number
7. ve range ve-range-number
8. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

Command or Action | Purpose
--- | ---
Device# configure terminal | Establishes a Layer 2 VPN (L2VPN) virtual forwarding interface (VFI) for specifying core-facing pseudowires in a Virtual Private LAN Services (VPLS) and enters L2VFI configuration mode.

#### Step 3

**l2vpn vfi context vfi-context-name**  
**Example:**
Device(config)# l2vpn vfi context vfi1

> • The VFI represents an emulated LAN or a VPLS forwarder from the VPLS architectural model when using an emulated LAN interface.

#### Step 4

**vpn id vpn-id**  
**Example:**
Device(config-vfi)# vpn id 10

> Configures a VPN ID for the VPLS domain.

#### Step 5

**autodiscovery bgp signaling bgp**  
**Example:**
Device(config-vfi)# autodiscovery bgp signaling bgp

> Enables BGP auto-discovery and BGP signaling on the device.

#### Step 6

**ve id ve-ID-number**  
**Example:**
Device(config-vfi)# ve id 1

> Configures a VPLS Endpoint ID (VEID) for the NLRI exchanged between BGP devices for BGP auto-discovery with BGP signaling.

> • For example, VEID numbering sequences such as 1,2,3 or 501, 502, 503 are preferred because the VEIDs are contiguous.

> • Avoid a non-contiguous numbering scheme such as 100, 200, 300.

> Repeat this step to add more VEIDs. The VEID must be unique within the same VPLS domain for all PE devices.

> **Note**  
> If you change the VEID, then the virtual circuit (VC) reprovisions and traffic is impacted as a result.

#### Step 7

**ve range ve-range-number**  
**Example:**
Device(config-vfi)# ve range 10

> Overrides the minimum size of VPLS edge (VE) blocks.

> • The VE range value should be approximately the same as the number of neighbors (up to 100).

> • The VE range can be configured based on the number of neighboring PE devices in the network.

> • For example, if 50 PE devices are in a VPLS domain, then a VE range of 50 is better than 10 because the number of NLRI exchanged are less and the convergence time is reduced.
If no VE range is configured or an existing VE range value is removed, then the default VE range of 10 is applied. The default VE range should not be used if the device has many PE neighbors.

Note: If you change the VE range, then the VC reprovisions and traffic is impacted as a result.

**Step 8**

**Example:**

Device(config-vfi)# end

Exits L2 VFI configuration mode and returns to privileged EXEC mode.

Note: Commands take effect after the device exits L2VFI configuration mode.

---

**Configuring BGP Signaling for VPLS Autodiscovery**

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `router bgp autonomous-system-number`
4. `bgp graceful-restart`
5. `neighbor {ip-address | peer-group-name} remote-as autonomous-system-number`
6. `address-family l2vpn vpls`
7. `neighbor {ip-address | peer-group-name} activate`
8. `neighbor {ip-address | peer-group-name} send-community extended`
9. `neighbor {ip-address | peer-group-name} suppress-signaling-protocol ldp`
10. `exit-address-family`
11. Repeat steps 1 to 10 to configure and activate other BGP neighbors in an L2VPN address family.
12. `end`
13. `show l2vpn vfi`
14. `show ip bgp l2vpn vpls {all [summary] | rd route-distinguisher}`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
| `enable`
| **Example:**
| Device> enable |
| Enables privileged EXEC mode.
| • Enter your password if prompted. |
| **Step 2**
| `configure terminal`
| **Example:**
<p>| Device# configure terminal |
| Enters global configuration mode. |</p>
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td><strong>router bgp</strong> autonomous-system-number</td>
<td>Enters router configuration mode for the specified routing process.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# router bgp 100</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><strong>bgp graceful-restart</strong></td>
<td>Enables the Border Gateway Protocol (BGP) graceful restart capability globally for all BGP neighbors.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-router)# bgp graceful-restart</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><strong>neighbor</strong> {ip-address</td>
<td>peer-group-name} remote-as autonomous-system-number</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-router)# neighbor 198.51.100.1 remote-as 65000</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td><strong>address-family l2vpn vpls</strong></td>
<td>Specifies the L2VPN address family and enters address family configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-router)# address-family l2vpn vpls</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td><strong>neighbor</strong> {ip-address</td>
<td>peer-group-name} activate</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-router-af)# neighbor 198.51.100.1 activate</td>
<td></td>
</tr>
<tr>
<td>Step 8</td>
<td><strong>neighbor</strong> {ip-address</td>
<td>peer-group-name} send-community extended</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-router-af)# neighbor 198.51.100.1 send-community extended</td>
<td></td>
</tr>
<tr>
<td>Step 9</td>
<td><strong>neighbor</strong> {ip-address</td>
<td>peer-group-name} suppress-signaling-protocol ldp</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-router-af)# neighbor 198.51.100.1 suppress-signaling protocol ldp</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------</td>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>10</td>
<td>exit-address-family</td>
<td>Exits address family configuration mode and returns to router configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-router-af)# exit-address-family</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Repeat steps 1 to 10 to configure and activate other BGP neighbors in an L2VPN address family.</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>end</td>
<td>Exits router configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-router)# end</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>show l2vpn vfi</td>
<td>Displays information about the configured VFI instances.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# show l2vpn vfi</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>show ip bgp l2vpn vpls {all [summary]</td>
<td>Displays information about the L2VPN VPLS address family.</td>
</tr>
<tr>
<td></td>
<td>[route-distinguisher]}</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# show ip bgp l2vpn vpls all summary</td>
<td></td>
</tr>
</tbody>
</table>
**Configuration Examples for L2VPN VPLS Inter-AS Option B**

**Example: VPLS BGP Signaling L2VPN Inter-AS Option B**

The following example configuration describes Inter-AS Option B for VPLS BGP signaling in a Layer 2 VPN. BGP MPLS forwarding is required between ASBR 1 and ASBR 2.

**Note**

From a BGP signaling perspective, there is no specific change within the autonomous system. From the VPLS perspective, there is EBGP peering between ASBR1 and ASBR2.

The following figure shows a network diagram for the BGP signaling Inter-AS option B BGP configuration:

*Figure 1: VPLS BGP Signaling L2VPN Inter-AS Option B Sample Topology*

The following example shows the PE 1 BGP configuration for Inter-AS Option B:

```
12vpn vfi context TEST101
vpn id 1
autodiscovery bgp signaling bgp
```
ve id 1
route-target import 22:22
route-target export 11:11
no auto-route-target
!
mls ldp graceful-restart
!
bridge-domain 1
member GigabitEthernet0/0/7 service-instance 101
member vfi TEST101
!
interface Loopback0
  ip address 198.51.101.2 255.255.255.255
!
interface GigabitEthernet0/0/1
  description - connects to RR1
  ip address 200.1.1.1 255.255.255.0
  negotiation auto
  mpls ip
!
interface GigabitEthernet0/0/7
  description - connects to CE1
  no ip address
  negotiation auto
  service instance 101 ethernet
  encapsulation dot1q 101
  rewrite ingress tag pop 1 symmetric
!
!
router ospf 10
nsf
network 200.1.1.0 0.0.0.255 area 0
network 198.51.101.2 0.0.0.0 area 0
!
router bgp 10
bgp log-neighbor-changes
bgp update-delay 1
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
no bgp default ipv4-unicast
neighbor 200.1.1.1 remote-as 10
neighbor 200.1.1.1 update-source Loopback0
!
address-family ipv4
exit-address-family
!
address-family l2vpn vpls
neighbor 200.1.1.1 activate
neighbor 200.1.1.1 send-community extended
neighbor 200.1.1.1 suppress-signaling-protocol ldp
exit-address-family
!

The following example shows the ASBR 1 BGP configuration for Inter-AS Option B:

router bgp 10
bgp log-neighbor-changes
bgp update-delay 1
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
no bgp default ipv4-unicast
no bgp default route-target filter
neighbor 192.0.2.1 remote-as 10
neighbor 192.0.2.1 update-source Loopback0
neighbor 203.0.203.1 remote-as 20
neighbor 203.0.203.1 ebgp-multihop 255
neighbor 203.0.203.1 update-source Loopback0
!
address-family ipv4
   exit-address-family
!
address-family l2vpn vpls
neighbor 192.0.2.1 activate
neighbor 192.0.2.1 send-community extended
neighbor 192.0.2.1 next-hop-self
neighbor 192.0.2.1 suppress-signaling-protocol ldp
neighbor 203.0.203.1 activate
neighbor 203.0.203.1 send-community extended
neighbor 203.0.203.1 next-hop-self
neighbor 203.0.203.1 suppress-signaling-protocol ldp
exit-address-family

The following example shows the ASBR 2 BGP configuration for Inter-AS Option B:

mpls ldp graceful-restart
!
interface Loopback0
   ip address 203.0.203.1 255.255.255.255
!
interface GigabitEthernet0/0/1
   description - connects to RR1
   ip address 192.0.2.2 255.255.255.0
   negotiation auto
   mpls ip
   mpls bgp forwarding
!
interface GigabitEthernet0/2/1
   description - connects to ASBR3
   ip address 192.0.2.200 255.255.255.0
   negotiation auto
   mpls ip
   mpls bgp forwarding

router ospf 10
   nsf
   network 192.0.2.0 0.0.0.255 area 0
   network 203.0.203.1 0.0.0.0 area 0
   network 0.0.0.0 255.255.255.255 area 0
!
router bgp 10
   bgp log-neighbor-changes
   bgp update-delay 1
   bgp graceful-restart restart-time 120
   bgp graceful-restart stalepath-time 360
   bgp graceful-restart
   no bgp default ipv4-unicast
   no bgp default route-target filter
   neighbor 203.0.203.3 remote-as 20
   neighbor 203.0.203.3 ebgp-multihop 255
   neighbor 203.0.203.3 update-source Loopback0
   neighbor 203.0.203.2 remote-as 10
   neighbor 203.0.203.2 update-source Loopback0
!
address-family ipv4
   exit-address-family
!
address-family l2vpn vpls
neighbor 203.0.203.3 activate
The following example shows the PE 2 BGP configuration for Inter-AS Option B:

```conf
default
neighbor 203.0.203.3 send-community extended
neighbor 203.0.203.3 next-hop-self
neighbor 203.0.203.3 suppress-signaling-protocol ldp
neighbor 203.0.203.2 activate
neighbor 203.0.203.2 send-community extended
neighbor 203.0.203.2 next-hop-self
neighbor 203.0.203.2 suppress-signaling-protocol ldp
exit-address-family

default
VPLS BGP Signaling L2VPN Inter-AS Option B

Example: VPLS BGP Signaling L2VPN Inter-AS Option B

default
neighbor 203.0.203.3 send-community extended
neighbor 203.0.203.3 next-hop-self
neighbor 203.0.203.3 suppress-signaling-protocol ldp
neighbor 203.0.203.2 activate
neighbor 203.0.203.2 send-community extended
neighbor 203.0.203.2 next-hop-self
neighbor 203.0.203.2 suppress-signaling-protocol ldp
exit-address-family

The following example shows the PE 2 BGP configuration for Inter-AS Option B:

```

```conf
l2vpn vfi context TEST101
vpn id 1
autodiscovery bgp signaling bgp
ve id 2
  route-target import 22:22
  route-target export 11:11
  no auto-route-target

mpls ldp graceful-restart

bridge-domain 1
  member GigabitEthernet0/0/7 service-instance 101
  member vfi TEST101

interface Loopback0
  ip address 192.0.2.3 255.255.255.255

interface GigabitEthernet0/0/1
  description - connects to RR1
  ip address 192.0.2.1 255.255.255.0
  negotiation auto
  mpls ip

interface GigabitEthernet0/0/7
  description - connects to CE2
  no ip address
  negotiation auto
  service instance 101 ethernet
  encapsulation dot1q 101
  rewrite ingress tag pop 1 symmetric

router ospf 10
  nsf
  network 192.0.2.0 0.0.0.255 area 0
  network 192.0.2.3 0.0.0.0 area 0

router bgp 10
  bgp log-neighbor-changes
  bgp update-delay 1
  bgp graceful-restart restart-time 120
  bgp graceful-restart stalepath-time 360
  bgp graceful-restart
  no bgp default ipv4-unicast
  neighbor 211.1.1.1 remote-as 10
  neighbor 211.1.1.1 update-source Loopback0
  address-family ipv4
  exit-address-family

address-family l2vpn vpls

neighbor 211.1.1.1 activate
neighbor 211.1.1.1 send-community extended
```
neighbor 211.1.1.1 suppress-signaling-protocol ldp
exit-address-family

The following example shows the route reflector device BGP configuration for Inter-AS Option B:

```
neighbor 211.1.1.1 suppress-signaling-protocol ldp
exit-address-family

mpls ldp graceful-restart
!
interface Loopback0
  ip address 203.0.203.1 255.255.255.255
!
interface GigabitEthernet1/1
  description - connects to PE1
  ip address 203.0.203.2 255.255.255.0
  mpls ip
!
interface GigabitEthernet1/2
  description - connects to PE2
  ip address 203.0.203.3 255.255.255.0
  mpls ip
!
interface GigabitEthernet1/5
  description - connects to ASBR1
  ip address 203.0.203.4 255.255.255.0
  mpls ip
  mpls bgp forwarding
!
interface GigabitEthernet1/6
  description - connects to ASBR2
  ip address 203.0.203.5 255.255.255.0
  mpls ip
  mpls bgp forwarding
!
router ospf 10
  nsf
  network 203.0.203.6 0.0.0.255 area 0
  network 203.0.203.7 0.0.0.255 area 0
  network 203.0.203.8 0.0.0.255 area 0
  network 203.0.203.9 0.0.0.255 area 0
!
router bgp 10
  bgp log-neighbor-changes
  bgp update-delay 1
  bgp graceful-restart restart-time 120
  bgp graceful-restart stalepath-time 360
  bgp graceful-restart
  no bgp default ipv4-unicast
  neighbor 203.0.203.11 remote-as 10
  neighbor 203.0.203.11 update-source Loopback0
  neighbor 203.0.203.12 remote-as 10
  neighbor 203.0.203.12 update-source Loopback0
  neighbor 203.0.203.13 remote-as 10
  neighbor 203.0.203.13 update-source Loopback0
  neighbor 203.0.203.14 remote-as 10
  neighbor 203.0.203.14 update-source Loopback0
!
address-family ipv4
  exit-address-family
  !
address-family l2vpn vpls
  neighbor 203.0.203.11 activate
  neighbor 203.0.203.11 send-community extended
  neighbor 203.0.203.11 route-reflector-client
  neighbor 203.0.203.11 suppress-signaling-protocol ldp
  neighbor 203.0.203.12 activate
```
neighbor 203.0.203.12 send-community extended
neighbor 203.0.203.12 route-reflector-client
neighbor 203.0.203.12 suppress-signaling-protocol ldp
neighbor 203.0.203.13 activate
neighbor 203.0.203.13 send-community extended
neighbor 203.0.203.13 route-reflector-client
neighbor 203.0.203.13 suppress-signaling-protocol ldp
neighbor 203.0.203.14 activate
neighbor 203.0.203.14 send-community extended
neighbor 203.0.203.14 route-reflector-client
neighbor 203.0.203.14 suppress-signaling-protocol ldp
exit-address-family
!

**Additional References for VPLS BGP Signaling L2VPN Inter-AS Option B**

**Related Documents**

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Command List, All Releases</td>
</tr>
<tr>
<td>MPLS commands</td>
<td>Multiprotocol Label Switching Command Reference</td>
</tr>
<tr>
<td>L2VPN VPLS Inter-AS Option B</td>
<td>L2VPN VPLS Inter-AS Option B</td>
</tr>
<tr>
<td>VPLS Autodiscovery: BGP Based</td>
<td>VPLS Autodiscovery BGP Based</td>
</tr>
<tr>
<td>VPLS BGP Signaling L2VPN Inter-AS Option A</td>
<td>VPLS BGP Signaling L2VPN Inter-AS Option A</td>
</tr>
</tbody>
</table>

**Standards and RFCs**

<table>
<thead>
<tr>
<th>Standard and RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>draft-kothari-l2vpn-auto-site-id-01.txt</td>
<td>Automatic Generation of Site IDs for Virtual Private LAN Service</td>
</tr>
<tr>
<td>draft-ietf-l2vpn-vpls-multihoming-03.txt</td>
<td>BGP based Multi-homing in Virtual Private LAN Service</td>
</tr>
<tr>
<td>RFC 6074</td>
<td>Provisioning, Auto-Discovery, and Signaling in Layer 2 Virtual Private Networks (L2VPNs)</td>
</tr>
<tr>
<td>RFC 4761</td>
<td>Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling</td>
</tr>
</tbody>
</table>
MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>• CISCO-IETF-PW-ATM-MIB (PW-ATM-MIB)</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
<tr>
<td>• CISCO-IETF-PW-ENET-MIB (PW-ENET-MIB)</td>
<td></td>
</tr>
<tr>
<td>• CISCO-IETF-PW-FR-MIB (PW-FR-MIB)</td>
<td></td>
</tr>
<tr>
<td>• CISCO-IETF-PW-MIB (PW-MIB)</td>
<td></td>
</tr>
<tr>
<td>• CISCO-IETF-PW-MPLS-MIB (PW-MPLS-MIB)</td>
<td></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>

Feature Information for VPLS BGP Signaling L2VPN Inter-AS Option B

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPLS BGP Signaling L2VPN Inter-AS Option B</td>
<td>Cisco IOS XE Release 3.12S</td>
<td>This feature simplifies the auto-discovery and signaling of all known provider edge (PE) devices in a VPLS instance by using BGP for both functions. The following command was modified: show mpls forwarding</td>
</tr>
</tbody>
</table>